OAO106 (Rev. 12/03) Affidavit for Search Warrant

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

ORDERED SEALED BY COURT

FILED

'05 SEP 29 AM 11: 19

CLERK, U.S. DISTRICT COURT SOUTHERN DISTRICT OF CALIFORNIA

BY: DEPUTY

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)
861 6TH AVENUE, SUITE 175, SAN DIEGO, CALIFORNIA

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Case Number: '05 mg 1561

I, ERIN D. KELLY being duly sworn depose and say:

I am a(n) Special Agent of the United States Department of Commerce and have reason to believe
Official Title

that ☐ on the person of or ☑ on the property or premises known as (name, description and/or location)
MAYSSAMI DIAMONDS, LOCATED AT 861 6TH AVENUE, SUITE 175, IN SAN DIEGO, CALIFORNIA, AS MORE PARTICULARLY DESCRIBED IN MY AFFIDAVIT WHICH IS ATTACHED HERETO

in the SOUTHERN District of CALIFORNIA

there is now concealed a certain person or property, namely (describe the person or property to be seized)
THOSE ITEMS SET FORTH WITH PARTICULARITY IN MY AFFIDAVIT, WHICH IS ATTACHED HERETO

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)
EVIDENCE OF A CRIME

concerning a violation of Title 50 United States code, Section(s) 1705(b); AND 18 USC 1956

The facts to support a finding of probable cause are as follows:
SEE MY AFFIDAVIT, WHICH IS ATTACHED HERETO

Continued on the attached sheet and made a part hereof: ☑ Yes ☐ No

E Kelly
Signature of Affiant

Sworn to before me and subscribed in my presence,

9/29/05 at SAN DIEGO, CALIFORNIA
Date City State

WILLIAM McCURINE, JR.
U.S. MAGISTRATE JUDGE
Name of Judge Title of Judge

W McCurine
Signature of Judge

IN THE MATTER OF THE SEARCH OF 861 6th AVENUE, SUITE 175, SAN DIEGO, CALIFORNIA	**AFFIDAVIT OF SPECIAL AGENT ERIN D. KELLY**

I. INTRODUCTION

I, Erin D. Kelly, am currently employed as a Special Agent by the Office of Export Enforcement (hereinafter "OEE"), Bureau of Industry and Security ("BIS") of the United States Department of Commerce. Being first duly sworn, I state as follows.

This affidavit is made in support of an application for a search warrant for Mayssami Diamonds, owned by Mohammad Ali Mayssami, located at 861 6th Ave., Suite 175, in San Diego, California. This location is further described below.

For reasons set forth below, I believe that there is probable cause to believe that evidence will be found at this location that pertains to the unlawful exportation of goods to the Islamic Republic of Iran, in violation of the International Emergency Economic Powers Act, codified at 50 U.S.C. §§ 1701 *et seq.*; the Export Administration Act, codified at 50 App. U.S.C §§ 2401 *et seq.*, as well as related Export Regulations found at 15 C.F.R. §§ 730 *et. seq.*; the Iranian Transactions Regulations found at 31 C.F.R. §§ 560 *et seq.*; and of money laundering in violation of 18 U.S.C. § 1956. As set forth below, I believe that there is probable cause to believe that evidence of money laundering will be found as well as evidence that Mayssami aided in the illegal exports by facilitating payment from Iran to the U.S. for the exports.

II. TRAINING AND EXPERIENCE

I am a Special Agent assigned to the San Jose Field Office of the Office of Export Enforcement. I am a law enforcement officer of the United States within the meaning of 18 U.S.C § 2510(7), and I am authorized by law to conduct investigations and to make arrests for felony offenses.

I received a Master of Arts degree in Sociology/Criminology from California State University at San Jose in May of 1998. Prior to my position as a Special Agent with OEE, I was employed from October 1998 to October 2000 as a Special Investigator with a private company called U.S. Investigations Services, conducting background investigations of individuals seeking a federal security clearance.

I have been a Special Agent with OEE since November 2000. I graduated from the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, in February 2001. I have attended advanced training seminars in export investigations provided by OEE and BIS. I have participated in and conducted several investigations of violations of United States export laws and regulations.

As a result of my training and experience, I am familiar with federal laws and regulations relating to the export of "dual use" goods and technology from the United States. "Dual use" refers to items that have both a legitimate commercial use and a military use. This is explained in greater detail below. The laws that control the export of dual use goods and technologies include the Export Administration Act., 50 App. U.S.C. §§ 2401-2420, (hereinafter "EAA"), and the International Emergency Economic Powers Act 50 U.S.C. §§ 1701 *et seq.* (hereinafter, "IEEPA").

The statements contained in this affidavit are based on information I have learned through my personal participation in this investigation, as well as from oral and written reports of other law enforcement officers, from records, documents, and other evidence obtained during this investigation, and from my experience and training as a Special Agent with OEE. Since this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the authorization of the search warrant.

III. RELEVANT STATUTES AND REGULATIONS

A. Department of Commerce and Export Controls on Dual Use Items

The EAA authorized the Secretary of Commerce to regulate the export of items as necessary to protect the national security, foreign policy, nuclear non proliferation, and short supply[1] interests of the United States. The Secretary implemented the authority provided by the EAA through the Export Administration Regulations (hereinafter "EAR," or "Regulations") found at 15 C.F.R. §§ 730 *et. seq.*

The EAA expired on August 20, 2001. The President, however, utilized powers granted to him by the IEEPA to continue the Regulations in force. He did so via Presidential Executive Order 13222 of August 17, 2001 (3 C.F.R., 2001 Comp., p. 783), and extended it by Presidential Notice of August 2, 2005.

Title 50, United States Code, section 1705(b) makes it a crime to willfully violate any of the Regulations promulgated under IEEPA. The IEEPA also authorizes investigations into violations of Regulations. See 50 App. U.S.C.A. § 2411 (a)(1) and 50 U.S.C.A §§ 1702(a)(1), (2) and 1705(b).

The Secretary of Commerce is responsible for maintaining the Regulations, which, *inter alia*, identify items over which BIS exercises regulatory jurisdiction. Through the Regulations, BIS imposes a license or other export authorization requirement, including differing requirements to obtain a license, before certain items subject to the Regulations may be lawfully exported from the U.S. or lawfully re-exported from another country.

The Regulations establish a regulatory scheme that reflects the complexities of the security interests of the United States. For example, high end navigational components that may be useful in missile guidance systems will nonetheless be allowed to be exported to U.S. allies if certain licensing requirements can be met. On the other hand, certain low tech items will be banned from export to countries where human rights concerns exist. For example, the export of stun guns and handcuffs are heavily restricted to several countries, including China.

---

[1] "Short supply" refers to the Secretary's power to ban exports of commodities that are currently in short supply in the United States."

There are two components to the Regulations which, acting together, are the core of the this country's regulatory scheme to control the export of dual use items[2]. They are summarized below.

The first is the Commerce Control List (CCL). It is found at 15 C.F.R. § 774, Supp.1 The CCL establishes items subject to BIS licensing requirements. It includes technical specifications where necessary to sufficiently identify which items are covered. It also lists the reasons they are controlled for export. These reasons include, for example, nuclear non-proliferation (listed in the CCL as "NP"), antiterrorism (AT), and national security concerns (NS).

The CCL also assigns an Export Control Classification Number (ECCN) for each item specifically listed on the CCL.

There is another category of items that should be set forth. These are items that are subject to the EAR, but are not listed on the CCL. These are know as "EAR 99 items." These items are generally eligible for export without a license ("NLR" for "no license required") to virtually all destinations. However, EAR 99 items may not, with very limited exceptions, be exported to embargoed countries such as Iran.

The second component is the Country Chart, found at 15 C.F.R. § 738, Supp. 1. The Country Chart sets forth a list of countries down the left side of the page, and a list of the reasons items are controlled for export (*e.g.*, non-proliferation, antiterrorism, *et cetera*) across the top of the page.

Thus, if the particular item is listed on the CCL as controlled for non proliferation reasons, and the country it is being sent to has an "x" in the non-

[2] There is a third component, not relevant to this search warrant application. It is the Entities List, found at 15 C.F.R. § 744, Supp. 4. This is a list of companies, organizations and government departments that may not receive certain specified items, even if others in the same country may do so.

proliferation box in the Country Chart, then the item generally requires a license to export[3].

The Regulations establish the responsibility of BIS, with the input from other federal agencies, to approve or deny export license requests for those items/country combinations that require a license. Persons wanting to send a product with an ECCN that is controlled to the destination country on the Country Chart, and for which no license exception applies, must first submit an export license application to BIS in Washington D.C. and receive approval of the license prior to export. Also, BIS may conduct pre license checks (PLCs) as part of the licensing process, at any foreign consignee identified on the license application as a recipient of the items to be exported. BIS may also establish licensing conditions to maintain control over the end-use of the item, including post shipment verifications (PSVs), which confirm if a commodity is actually being used as described in the export license.

15 C.F.R. § 764.2(C) provide that "No person may solicit or attempt a violation of the EAA, the Regulations, or any order, license or authorization issued thereunder."

15 C.F.R. § 764.2(d) provides that "No person may conspire or act in concert with one or more persons in any manner or for any purpose to bring about or to do any act that constitutes a violation of the EAA, the Regulations, or any order, license or authorization issued thereunder."

The Regulations also control the so-called "transshipment" of items subject to the Regulations, *i.e.*, the export of an item to an intermediate country, knowing that it's intended destination is actually a third country. Those seeking to circumvent U.S. export control laws often use intermediary countries to which items may be shipped without a license, and which impose limited or no controls on shipments of the applicable items to the third country. This is usually done to evade a ban on the export

[3] There are sometimes "license exceptions" provided in the EAR for specific items and countries which can remove the necessity for a license.

of the item to the third country, although proof of an intent to evade is not required to establish a violation of the Regulations. This is relevant to this case because of the apparent export of controlled items to the United Arab Emirates (U.A.E.) that were destined for Iran. (This is set forth at length below.)15 C.F.R. § 734.2(b)(6) provides:

> "For purposes of the Regulations, the export or reexport of items subject to the Regulations, that will be transshipped through a country or countries to a new country, or are intended for reexport to the new country, are deemed to be exports to the new country.

As mentioned above, willful violations of the IEEPA Regulations are criminal. 50 U.S.C. § 1705(b). The applicable United States Sentencing Guidelines is § 2M5.1.

B. The Department of Treasury and the Iranian Embargo

The United States Department of Treasury's Office of Foreign Assets Control (OFAC) administers the current trade embargo against Iran under the authority, *inter alia*, of IEEPA. The Department of the Treasury's Regulations implementing the embargo, "The Iranian Transaction Regulations" or "ITR," are found at 31 C.F.R. §§ 560 *et seq*.. They are separate from the Department of Commerce's regulations, although as set forth below, the two sets of regulations interact in several important respects.

On March 15, 1995, the President issued Executive Order 12957, finding the actions and policies of the Government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the U.S. On May 6, 1995, the President issued Executive Order 12959 that took additional steps to deal with Iran, and prohibited unauthorized exports from the U.S., transactions within the U.S., or by U.S. persons, that evade or avoid any of the prohibitions contained in the ITR.

The OFAC embargo and the ITR include prohibitions on the export and re-export to Iran of virtually all items on the CCL, as well as the export (including re-export) of EAR99 items to Iran.

The Department of Commerce regulations (the EAR) provide that export to Iran absent OFAC authorization is a violation of the EAR. See 15 C.F.R. § 746.7. This is true even for items classified as EAR 99 which could otherwise be lawfully exported to Iran.

C. Money Laundering

18 U.S.C., § 1956(a)(2) makes it illegal for, *inter alia*, a person to move money from the U.S. to another country, or from another country to the U.S., with either (1) the intent to promote a "specified unlawful activity;" (SUA) or (2) with knowledge that the funds are the proceeds of "some form of unlawful activity" if the person has knowledge that the movement of the funds is designed to conceal the nature, location or source of the SUA.

Violations of "section 206 (relating to penalties) of the International Emergency Economic Powers Act" [50 U.S.C. § 1506] constitute a "specified unlawful activity" for the purposes of money laundering. 18 U.S.C § 1956(c)(7)(D). This reference in the money laundering statute makes violations of both the EAR and the ITR "specified unlawful activit[ies].".

IV. PROBABLE CAUSE

A. Export investigation of Supermicro Computer Inc.

In May of 2003, I began an investigation into the export activities of Supermicro Computer Inc. ("Supermicro"), located at 980 Rock Avenue, in San Jose, California. I did so because an anonymous source contacted the BIS Website to report concerns about possible diversions of U.S.-origin computer equipment to Iran. The source then contacted me by phone and email, alleging that Supermicro, a U.S. company that manufactures printed circuit boards and computer hardware and software, was engaging in illegal exports to Iran. The source told me that Supermicro was making illegal sales to Supernet Computers LLC ("Supernet") and Aiden Company ("Aiden"), which are operated by Mr. Tofigh Setayeshi in the United Arab Emirates (U.A.E.) and Iran, respectively. The source said he/she was telling us this because he/she was a law abiding competitor of Supernet, and found it very difficult to compete with Supernet when they were illegally importing Supermicro products.

According to a Dun & Bradstreet business report, Supermicro is incorporated in the state of California and employs approximately 90 people in the U.S. and Asia. Supermicro has one subsidiary, Supermicro Computer BV in The Netherlands. It also has two sister companies called Supermicro (Asia) and Ablecom Technology, which are both located in Taiwan. Supermicro also has distributors and re-sellers in more than 30 countries. Supermicro has sales in excess of $80 million per year.

Supermicro manufactures and sells numerous commodities which are subject to the Regulations. According to BIS licensing officers, Supermicro's motherboards were controlled under ECCN's 4A003.b and 4A994.b for National Security (NS) and Anti-Terrorism (AT) reasons at the time of the exports described below. Supermicro's computer chassis' are also subject to the EAR, classified as EAR99, *i.e.* exportable to most locations with no license required (NLR), but not to Iran because of the embargo.

Exporters routinely use a form letter called a Shipper's Letter of Instructions. This is a form used by a shipper to inform a freight forwarder how and where to ship the exports. The form has a box on it for the ECCN.

There is reason to believe that Supermicro knew about the EAR and knew that some of their products are controlled for export purposes. Their Shipper's Letter of Instructions from 2002, for shipments including Supermicro motherboards, correctly list the ECCN as either "4A003" or "4A994".

In February and August of 2004, Supermicro was served with two administrative subpoenae from the Department of Commerce, requiring that it produce documents relating to its exports to Supernet in the U.A.E. and Aiden in Iran.

I have reviewed the documents produced pursuant to those subpoenae. They included email communications between Setayeshi (doing business as Supernet and Aiden) and Supermicro employees Annie Hoang-Ai Truong and Robbie J. Abreu. I also interviewed Supermicro employees, including Abreu and Truong.

Based on the subpoenaed documents and the interviews, I learned that, on April 9, 2001, Charles Liang, the CEO of Supermicro, and Mohsen Vakily Roboty, representing Supernet Computers LLC in Dubai, U.A.E., signed a business agreement appointing Supernet as a Supermicro non-exclusive distributor in the U.A.E., and an exclusive distributor in Iran. Annie Truong was the Supermicro Sales Account Manager responsible for the Supernet/Setayeshi account, and Abreu was the Vice President in charge of sales and was also Truong's supervisor.

Various e-mails I reviewed show that Truong and Abreu had reason to know about the U.S. embargo against Iran. In one email, on November 25, 2002, Truong e-mailed Setayeshi regarding her attempt to send documents to Setayeshi in Iran. She said "FedEx and UPS told us they don't have a destination to Iran."

In a February 4, 2002, email from Abreu to Setayeshi, Abreu states "...we can't sell direct to Iran due to the embargoes from the USA."

Additionally, an email between Truong and another foreign customer, on August 22, 2002, shows that Truong had reason to know that Iran was a restricted destination. The customer stated, "I want to ship the container directly to Iran so I have to not buy it FOB[4] because you can't ship it to my destination." Because of the Iranian embargo, shipments are not allowed from the U.S. to Iran, so the seller would either have to ship the items to another destination besides Iran or the seller would have to name Iran as the destination and release the goods to that destination in order to ship under FOB (which would immediately cause the shipment to be flagged and, most likely, detained and inspected).

In April 2003, after the confidential informant contacted Supermicro in writing and threatened to notify the Department of Commerce regarding allegations that Setayeshi was selling Supermicro's products in Iran illegally, Truong contacted Setayeshi. I have reviewed the emails. In an interview, Truong told me they also talked

[4]The term FOB, which stands for either Free on Board or Freight On Board, is an international term of sale in which the exporter/seller fulfills his or her obligation to deliver when the goods have passed over the ships rails at the port it is being shipped from. Once the goods are on board the buyer must accept all risks of loss or damage to the goods from that point forward. FOB requires that the seller/exporter clear the goods for export.

via telephone about the issue.

On April 11, 2003, Setayeshi e-mails Truong and states "...it is clear that it is Golden System is the one who had sent the documents to Mr. Charles [Liang]..." to which Truong replies "please let me know if your person find out anything about Golden System...I didn't have any idea about how we can do to stop this. Basically, I believe that they will not do anything to harm our company. It's only a threat."

Three days later, on April 14, 2003, Setayeshi replies and suggests a plan to try to conceal the fact that Supermicro products are being sold in Iran. He wrote "I have not any information what really they will do with SM [Supermicro] and their documents. But I believe it would be better we would care the same and do any precautions needed. So they cannot proof anything...for example, I will not send you any email in the aiden@jamejam.net but I will send it in the snet@emirates.net and will not use the holograms in the name of Supernet and Aiden together anymore...this way they can not proof anything against Supermicro."

Three days later, on April 17, 2003, Truong e-mails Setayeshi and indicates that she thinks the threat is over and that she plans to continue to sell products to Iran. She wrote "So far everything seems to be quiet. I guess it's only a threat...Please let me know how is the market in Iran and Dubai."

B. Export violations uncovered during investigation of Supermicro Computer Inc.

My review of purchase orders, invoices, email communications, and various financial documents such as accounts receivable reports and copies of deposit confirmations, revealed that Supermicro and Setayeshi engaged in several legal transactions involving sales of Supermicro equipment to Setayeshi for sale in the U.A.E. Those records also indicate, however, that Supermicro and Setayeshi knowingly engaged in the illegal transfer and reexport of various Supermicro commodities controlled by the EAR to Iran on fifteen occasions between 2001 and 2004. For the purposes of this search warrant, and in the interests of being succinct, only five of those fifteen violations will be discussed below.

I checked the Department of Commerce's BIS licensing data base. Neither Supermicro or Setayashi have applied for nor received an export license. I also checked with OFAC and they reported back to me that Supermicro had not applied for nor received permission to export anything to Iran.

Also, as will be seen in the details included below, four of the five violations appear to involve money laundering through an alternative banking system known as "hawala." Three of the five violations noted included the use of hawala by Mohammad Ali Mayssami. Before setting forth the evidence of the export violations, a brief explanation of hawala will be provided.

C. Money Laundering and Hawala

In November of 2004, I requested that Special Agent Mary Hicok of the Department of the Treasury, Internal Revenue Service, Criminal Investigation (IRS-CI), join the investigation of Supermicro. I did this because evidence of possible money laundering violations had surfaced.

On August 24, 2005, I spoke via telephone with Elton Ellison, Senior Enforcement Investigations Officer, Office of Foreign Assets Control (OFAC). OFAC is the federal agency responsible for administering the economic and trade sanctions against Iran.

According to Mr. Ellison, under the Iranian Transaction Regulations (ITR), 31 C.F.R. §§ 560 *et seq.*, depository (*i.e.*, banking) institutions in the U.S. can transfer money in and out of Iran only if the money is for non-commercial purposes or transactions, such as humanitarian reasons, or a gift. If a person, no matter where he or she was located, arranged for an Iranian bank to transfer money to a U.S. bank, the U.S. bank would be required under the ITR to ask what the purpose of the transfer was. If it was for a commercial transaction, the U.S. bank would be required to deny the transfer. This would make it nearly impossible for Setayeshi to transfer money from Iran to the U.S.

I explained the financial information I had reviewed during the Supermicro investigation, described below. Mr. Ellison told me that the payment strategy used by Supermicro with Setayeshi and Mayssami sounded like "hawala".

Hawala is defined by one author as an alternative, or parallel, remittance system that exists and operates outside of traditional banking or financial channels.[5] Hawala is used by individuals around the world to finance both legal and illegal transactions.

According to Mr. Ellison, hawala has been around for a long time, but came to the attention of U.S. investigators after the September 11, 2001, attacks because of the use of hawala in financing terrorism.

According to Jost and Sandhu's article, hawala is built on trust and community ties, and makes use of individual relationships and "regional connections". Hawala originated hundreds of years ago, prior to traditional banking practices, and is used widely today throughout the world. Hawala is frequently referred to as "underground banking," which can be misleading because the system often operates legally and in the open, with its services heavily advertised.

According to another author, Robert E. Looney,[6] investigators can no longer rely solely on commercial banking records and data for investigations into "funding mechanisms" of certain criminal conduct, because other systems such as hawala can be used. Looney explains hawala as "a transfer or remittance from one party to another, without use of a formal financial institution such as a bank or money exchange, and is, in this sense, an 'informal transaction.' "

Hawala transactions are conducted through a network of hawala brokers, known as hawaladars. An individual wishing to get money to a destination through the use of the hawala network would contact a hawaladar in one city and give them the amount of money they wish to transfer. The hawaladar then contacts a hawala broker in the city the money is to be transferred to (usually a foreign city) and provides them with details of the transfer. Rarely is any money exchanged between the two hawaladars. A hypothetical example of a hawala transaction follows.

---

[5] "The Hawala Alternative Remittance System and its Role in Money Laundering" by Patrick M. Jost and Harjit Singh Sandhu, Interpol General Secretariat, Lyon France, January 2000. An electronic version of the article can be found online at http://www.interpol.int/Public/FinancialCrime/MoneyLaundering/hawala/default.asp

[6] Robert E. Looney in "Following The Informal Money Trail: The Hawala Financial Mechanism" (*Strategic Insights*, Volume 1, Issue 9, November 2002. Published by the U.S. Naval Postgraduate school.) This article is available at http://www.ccc.nps.mil/si/nov02/southasia.asp

> A business owner in Dubai, U.A.E., wishes to send $1,000.00 to his cousin in Los Angeles, California. He contacts his local hawaladar and gives him $1,000.00 or the equivalent in U.A.E. Dirhams. The U.A.E. hawaladar then contacts a hawaladar in the Los Angeles area. The Los Angeles hawaladar gives $1,000.00 to the cousin out of his (the L.A. hawaladar's) own funds. No money is actually exchanged between the two hawaldars. The $1,000.00 given to the U.A.E. hawaladar stays in the U.A.E. hawaldar's possession. Consequently, the U.A.E. hawaladar now owes the Los Angeles hawaldar $1,000.00. He promises the Los Angeles hawaladar that he will settle the debt for $1,000.00 with the Los Angeles hawaladar at a later date – usually when someone in Los Angeles wants to send money to the U.A.E.

> If the U.A.E. hawaladar does not know any other hawaladars in Los Angeles, he or she will generally contact another hawaladar in the U.S. that they know and they will either refer them to someone in the Los Angeles area or handle the transaction themselves from outside the Los Angeles area. Hawaladars do not need to be in the same city or state as the recipient of the money because funds can always be sent domestically via wire transfer, check or money order.

Not all hawala transactions will be done in exactly the manner set forth in the above hypothetical.

The most unique characteristics of hawala transactions are that hawaladars seldom use any written promissory instruments. It is based on trust. And the exchanges are not monitored or regulated by local government. It is all done through the honor system. Because it is based on trust it is often viewed as a safe, secure and quick way to transfer funds.

The re-payment of a debt from one hawaladar to another can take many forms and may not always be a direct cash re-payment. Hawaladars usually make a profit by charging a small commission, or by using slightly advantageous exchange rates between currencies.

As set forth below, documents received pursuant to the administrative subpoenae show that during the time that the violations of the export laws were committed, Setayeshi frequently transferred funds from banks in the U.A.E. to Supermicro's U.S. bank account, Bank of America Account number 0011863-19219, for purchases of Supermicro equipment. It is legal to transfer money from the U.A.E. to the U.S.

But the records also show that when Setayeshi wanted to send money from *Iran* for the illegally exported products, he arranged for Mr. Mayssami or others in the U.S. to make payment to Supermicro.

D. Specific transactions involving Supermicro, Supernet and Mayssami

As mentioned above, Mayssami provided U.S. funds for three of the transactions between Supernet and Supermicro at the request of Setayeshi. The details of those three transactions are discussed below.

It is important to understand that, as will be seen below, Setayashi would often place money on account with Supermicro, in advance of making a particular order. He did this both through legitimate banking transactions from the U.A.E. as well as hawala deposits from Mayssami. When he placed an order with Supermicro, the cost would be deducted from his account. If he didn't have enough money in his account to cover the order, Supermicro would ask him to deposit some more money before the order would be released for shipment. Because of this, the amounts of the deposits did not always match exactly the amount of the order.

Violation 1

I have reviewed several documents obtained from Supermicro regarding a sale, in January 2002, of four hundred motherboards, for $36,800.00, and controlled under ECCN 4A003.b. The documents included a purchase order, an invoice, and several e-mails regarding payment for the transaction. Supermicro Invoice number IN0898516, dated January 29, 2002, shows the sale of 400 P4SBA+ motherboards to Supernet in Dubai, U.A.E. According to the invoice, the shipping address for the sale is Aiden Company Ltd., No. 85, 30th Tir, Jomhoori Avenue, Tehran, Iran. Shipping documents and e-mails between Truong and Setayeshi show that the order was shipped on Supermicro's behalf by Wistron Corporation in Hong Kong to Bar Baran Iran International Forwarding company in Tehran, Iran, on January 25, 2002.

One of the e-mails I reviewed was sent on January 23, 2002, by Setayeshi to Truong and states "...I talked to Mr. Mehrdad on his mobile (001 619 70 88 884)[7] and he informed me that he has transfer[r]ed $50 000 to your account and is faxing you the document." Truong replies to Setayeshi, saying "Mr. Mayssami already called me, and he faxed over to me the deposit confirmation."

Supermicro also provided a copy of a Bank of America deposit confirmation, dated the same date as the email, *i.e.*, January 23, 2002, which shows that a $50,000.00 deposit was made to Supermicro's account, account number 0011863-19219, with a routing transit number of 540930135.

In July 2005, Special Agent Hicok and I obtained additional bank records via grand jury subpoena. These records showed that a personal check from one Reza Paydar, in the amount of $50,000.00, was deposited directly into Supermicro's account at Bank of America. The date on the check was the same date that Mayssami made the deposit to Supermicro, January 23, 2002. Paydar's address on the check was listed as 7855 Herschel Avenue, Suite 201, La Jolla, California. The telephone number on the check was (619) 456-9201. It was a personal check numbered 1018.

Based on this, as well as the violations set forth below, it appears that Mayssami, while in San Diego, was depositing money into Supermicro's account to cover Setayeshi's debt to Supermicro. As will become more apparent below, it also appears that Mayssami is not using money he receives from Setayeshi for this purpose. He is using his own money, received from his jewelry and other customers.

---

[7] As set forth later, telephone company records establish that this telephone number is assigned to Mr. Mayssami. We do not know why Setayashi refers to him as "Mehrdad" sometimes and "Meisami" at other times. But it is clear from the telephone number as well as Truong's response ("Mr. Mayssami already called me...") that "Mehrdad" is Mohammad Mayssami.

But he is not depositing his own money in his own name – say, a check from his own checking account. Instead he is depositing checks from his customers or business associates, made payable to Supermicro. This is an apparent attempt to conceal that the payments are "proceeds from some form of unlawful activity," *i.e.*, payment for illegal exports to Iran.

Violation 2

Supermicro invoice number IN0904734, dated May 7, 2002, shows that Supermicro sold 1,000 motherboards, valued at $71,540.00, and controlled under ECCN 4A994.b, to Supernet in Dubai, U.A.E. Although the invoice shows Supernet in Dubai as the "Bill To" and "Ship To" address, a Special Price Agreement signed by Charles Liang on April 19, 2002, authorizes a reduced price for the motherboards for Supernet in order "to win Dubai and Iran market." A Shipper's Letter of Instructions from Supermicro shows that the order was shipped from Supemicro in San Jose, California to Supernet in Dubai on May 7, 2002.

Included among documents reviewed regarding this order were several e-mails between Abreu, Truong, Setayeshi and Liang negotiating the price for the motherboards. An e-mail from Setayeshi to Truong on April 19, 2002, states "I am sure this product with $45 price will make SM win over Gigabyte in Iran and change the market in favor of us." On subsequent dates, Abreu e-mails Liang for approval of the $45 price requested by Setayeshi and Liang responds to the e-mail on April 22, 2002, saying "we may offer at $60 for 500 pcs or more".

An e-mail from Truong to Setayeshi on April 19, 2002, states "...the accounting told me you don't have enough credit in your account" to which Setayeshi responds "It seems about $1100 is shorted. It is not possible for me to send any money today, because both in Iran and Dubai, Friday is off day and closed...I will send $50 000 or $60 000 next week to start the main order." Truong responds on the same day that she will guarantee the funds with accounting so the order is released and they will wait until Monday (April 22nd) for payment from Setayeshi.

On May 6, 2002, Setayeshi sends Truong an email stating "Please also get the confirmation of $5000 and $11000 of direct deposit of Mr. Meisami and let me know?"

Special Agent Hicok and I obtained and reviewed bank records via grand jury subpoena which show a deposit to the Supermicro Bank of America account on April 26, 2002, of ten (10) Western Union Money Orders valued at $500 each, totaling $5,000.00, one of the amounts mentioned by Setayeshi in the May 6 email. The serial numbers of the money orders were: 06-479615807 through 809, 06-479615812, 06-310353422 and 06-310353430 through 434. The name Supermicro Computer is hand written in as the payee on each money order and each money order is signed with an illegible signature. No purchaser address was provided on any of the money orders.

Special Agent Hicok and I obtained and reviewed bank records via grand jury subpoena. They show that a personal check dated May 2, 2002, in the amount of $1,100.00 from the account of Julie R. Rampoldi, 2437 Mission St., Escalon, CA, was part of a deposit made into Supermicro's account on May 6, 2002. Two additional personal checks, each for the amount of $3,000.00, both written by David Hughey (one showing a Gilroy, CA address, the other a Memphis, TN address) on May 3, 2002, were also part of the same deposit. Records show that $3,900.00 cash was also deposited. The total amount deposited was, therefore, $11,000.00 – the other amount mentioned by Setayeshi in the May 6, 2002, email. As mentioned, the deposit was made on May 6, 2002.

On August 22, 2005, Special Agent Hicok and I interviewed Julie R. Rampoldi via telephone. Rampoldi told me that she was not familiar with the name Supermicro Computer. I read Rampoldi the date, check number, amount and bank name that the check bearing her name was drawn on. Rampoldi stated that she had been in San Diego, California, in early May 2002, had become engaged to David Hughey, and purchased an engagement ring. Rampoldi stated that she did recall writing a $1,100.00 check, which was an advance on her credit card on her People's Bank account, at a jewelry store in San Diego. She could not recall who filled in the payee section, herself or Mayssami. Rampoldi also stated that Hughey (now her husband) wrote two checks at the jewelry store to cover the balance of the $7,100.00 cost of the engagement ring. Rampoldi did not recall the name of the jewelry store but did recall that the store was in a "jewelry mart".

Based on this, it appears clear that Julie Rampoldi and David Hughey bought a $7,100.00 engagement ring from Mayssami Diamonds on May 2 or May 3, 2002. They wrote three checks to cover the purchase. We do not know who filled in the payee section, but it is clear that the checks were not made payable to Mayssami Diamonds. They were instead made payable to Supermicro. It is clear that the checks were deposited by Mayssami into Supermicro's account to pay Setayeshi's debt to Supermicro for the illegal export to Iran that was shipped from San Jose, California on May 7, 2002, one day after the deposit.

Violation 3

According to Supermicro invoice number IN0913620, dated August 27, 2002, Supermicro sold 151 computer chassis', valued at $44,205.90 and subject to the Regulations, to Supernet. The invoice lists the billing address as Supernet in Dubai but the shipping address is Aiden Company, No. 85, First Floor, 30th Tir St., Jomhoori Avenue, Tehran, Iran. According to a fax cover sheet sent to Supermicro by the freight forwarder, Seven Ocean Maritime Transport Co Ltd in Taiwan, the shipment was scheduled to leave Keelung port in Taiwan on August 27, 2002, and arrive at Bandar Abbas port in Iran around September 9th (the arrival date is very difficult to read but appears to be "9/9"). Supermicro did not provide any other shipping documents for this shipment besides the fax confirmation from Seven Ocean, although an e-mail between Truong and Setayeshi on August 20, 2002, does confirm that the destination is the Bandar Abbas port in Iran.

An e-mail sent by Setayeshi to Truong on July 25, 2002, states "July 22 (I send an email for the TRN No.) Please check with accounting July 23 (I asked Mr. Meisami to fax it to you) please check with accounting" and further in the email states "...I asked Mr. Meisami to deposit $110 000 to SM account today." Truong's response states "We received $110,000.00 from Mr. Mayssami today. We're still checking on $20,000.00 direct deposit from him on July 22 and July 23."

Also included among the documentation reviewed regarding this order was a copy of a Bank One Wire Transfer request. According to the wire transfer documentation, $110,000.00 was transferred from Bank One account number 11564469 to Bank of America account number 11863-19219 on the same date as the email, *i.e.*, July 25, 2002. According to the paperwork reviewed, the customer of Bank One who had the bank make the transfer was Manouchehr Javadi, MJ Engineering Group, 3627 E Indian School Road, Suite 206, Phoenix, Arizona. The receiving beneficiary name is Supermicro Computer and hand written under "special instructions" it states "For Supernet Computer".

On August 11, 2005, Special Agent Hicok and I interviewed Manoucheher Javadi at M.J. Engineering Group, 3627 E Indian School Road, Suite 6, Phoenix, Arizona 85018. Javadi confirmed his signature on the wire transfer paperwork but stated that he did not know who Supermicro Computer was. Javadi told the investigators that the transfer was to purchase a condominium in Tehran, Iran, that he and his wife wanted to buy. But Javadi said he did not want to send money through the Iranian banks for fear that it would be stolen. Javadi reported that he contacted a "friend," named Hamid Hamedi who is a jeweler in the Los Angeles area. Hamedi found someone else who needed to get money to the U.S. from Iran – the opposite direction that Javadi needed his money to go – so they arranged for a trade. Javadi reported that he was told to send his $110,000 not to Tehran, but to Supermicro. He told us that he got the name and account number for Supermicro from Hamedi's friend, Mayssami. Javadi believes that Mayssami then arranged for Javadi's wife to receive $110,000.00 in Tehran. Javadi reported that this was a one-time transaction to help get money to Iran for the purchase of the condominium. Javadi stated that he did not recognize the names Supernet, Aiden Company or Setayeshi.

Mr. Elton Ellison at OFAC told me that he would need more facts to be sure, but it is possible that it might have been legal to conduct this transaction with Iran through traditional banking channels because the purchase of a house to use as your residence is not always considered a commercial transaction.

E. Additional violations not involving Mayssami

Violation 4

According to Supermicro Invoice number IN0892510, dated September 25, 2001, Supermicro sold one (1) Super Server 6011D valued at $578.20, one SC822S computer chassis (the box that houses the motherboard, power supply, drive bays, etc. in a computer) valued at $800.10 and one (1) Pentium 4 motherboard valued at $84.00 to Supernet Computers LLC, P.O. Box 43557, Dubai, U.A.E. The total value of the sale, including shipping, was $1,710.30. A Special Price Agreement (SPA) dated September 25, 2001, indicates that customer number SN0004 (Supernet's Customer ID number) should receive a price reduction on the three items because they "are samples for Trade show in Iran". The SPA request was made by Abreu and approved by Charles Liang, who initialed the Purchase Request Form.

An e-mail from Setayeshi (written from the aiden@jamejam.net e-mail address) to Abreu and Truong on September 6, 2001, states "As you know we will have a computer show in Iran at October, and we have just less than 20 days time. I need all your chassis and almost all models of motherboards...". The e-mail is signed "Tofigh

Setayeshi, Supernet Computers - DUBAI, Aiden Computers - IRAN". Shipping documents provided by Supermicro show that the shipment of the SC822S, 6011D Server and Pentium 4 motherboard were sent via Federal Express International Priority to Supernet's Dubai address on September 25, 2001. A Supermicro Accounts receivable spreadsheet and an e-mail from Truong to Setayeshi and Abreu on September 24, 2001, confirms that Supernet had a $9,249.43 balance in their account, enough to cover the cost of this shipment. At the time of this sale, Supermicro's Pentium 4 motherboards were controlled under ECCN 4A003.b and their chassis' were EAR99 and were not eligible for export or re-export to Iran without prior authorization from BIS or OFAC.

Violation 5

According to Supermicro Invoice number IN0892130, dated September 14, 2001, Supermicro sold twelve (12) SC830 computer chassis' valued at $5,266.00, thirty-eight (38) SC760 server chassis' valued at $7,220.00 and one-hundred thirty three (133) SC750 chassis' valued at $13,566.00 to Supernet Computers LLC, P.O. Box 43557, Dubai, U.A.E. The total value of the sale, including shipping and processing fees, was $26,554.00. An e-mail dated August 27, 2001, from Setayeshi (aiden@jamejam.net) to Abreu and Truong states "We should have them before oct. in tehran [Iran] and it takes more than 25 days sea shipping to Dubai and more than 10 days to Iran." Also included among the documentation regarding this sale is Ablecom Technology Inc. Invoice number 200951, also dated September 14, 2001. Ablecom Technology is a sister company to Supermicro Computer Asia and they are co-located at the same address with Supermicro Asia in Chung-Ho, Taipei, Taiwan. Ablecom Invoice 200951 contains the same 184 chassis products sold to Supernet by Supermicro on the same date, only the invoice states that Ablecom is selling the products to Supermicro Computer in San Jose, California. The invoice shows Supermicro's San Jose address as the "Bill To" and "Ship To" address for the sale, but a Vopak freight forwarding document dated September 19, 2001, shows that the shipment was shipped from Supermicro in Taiwan to Supernet in Dubai.

According to my interviews with Supermicro employees in San Jose and Ablecom employees in Taiwan, Ablecom and Supermicro Asia often manufacture and ship Supermicro's chassis orders from Taiwan to customers in Asia and the Middle East as it is cheaper than manufacturing and shipping only from the U.S. An e-mail from Setayeshi to Truong and Abreu on August 28, 2001, states "I faxed you a copy of 45000 USD TT[8] from Middle East Dubai today I hope you have received it yet, if so please let me know the exact received amount." Truong responds to Setayeshi on August 29, 2001, and says "Thank you, we received your TT. The exact amount is $44,983.00". A copy of the fax from Setayeshi to Truong shows that on August 27, 2001, $45,000.00 was transferred from Bank of America account number BW121000358 in San Jose, California under the name Tofigh Setayeshi, Dubai, U.A.E. to Supermicro's Bank of America, account number 11863-19219. Hand written on the fax it states "Attn: Mr. Tofigh - We are pleased to serve you." and it is signed with an illegible signature and stamp. Below that hand is also hand written "Dear Mrs. Annie; 8/29/001, This is the paper for 45000 USD from Middle East Bank of Dubai from: Supernet Dubai". This appears to be a hawala-type transaction because the money was transferred from one U.S. bank account to another U.S. bank account by an unnamed person who appears to have provided Bank of America with Setayeshi's name as the ordering customer. There is no indication that Mayssami was involved in this hawala transaction.

F. Additional banking documents

Special Agent Hicok and I analyzed bank records obtained via Grand Jury subpoena which indicate that on October 3, 2002, a deposit of $54,000.00 containing several personal checks and Western Union money orders was deposited into the Supermicro Bank of America account, account number 11863-19219. The address hand written on the Checking Deposit slip under the name "Super Micro Computer" is "861 6th Ave #175, SD, CA 92101" which is the address of Mayssami Diamonds. It is signed with an illegible signature. One of the checks included in the deposit records is a check in the amount of $5,000.00 from San Diego Jewelry and Loan, 933 5th Ave, San Diego, CA. Written in the bottom left corner of the check is a partially legible handwriting which says "Loan to Mr M......I". An e-mail dated October 4, 2002, from Setayeshi to Truong and Abreu states, "At last after a long time Mr. Meisami called me and told that he transfer[r]ed $59.000 yesterday."

---

[8] "USD" is a commonly used term for "United States dollars." "TT" is a commonly used term for a wire transfer.

G. Mohammad Ali Mayssami and Mayssami Diamonds

In several e-mails provided by Supermicro pursuant to administrative subpoena, Setayeshi refers to "my person" in California or a "friend" who will transfer money to Supermicro for payment on Setayeshi's behalf. Setayeshi provides limited information about the individual but occasionally refers to the "person" as "Mr. Meisami."

Mr. Setayeshi did, however, provide a cell phone number for his "friend" in California. On January 22, 2002, Mr. Setayeshi e-mailed Truong at Supermicro and told her that "Somebody in the name of Mr. Mehrdad will fax you a copy of $50 000...from CA. His mobile no. in the US is 001 619 70 88 884". The cell phone number appears to be an area code 619 number (the area code for San Diego), as one would have to dial it from overseas, *i.e.* 001 (the country code for the U.S.); then the area code, 619, and the local phone number, 708-8884.

In June of 2005, I issued an administrative subpoena to Cingular Wireless for phone number (619) 708-8884. According to Cingular Wireless, phone number (619) 708-8884 is registered to Mohammad Mayssami, at 861 6th Avenue, Suite 175, San Diego, California 92101, the address for Mayssami Diamonds.

A review of law enforcement and commercial databases including; Autotrack XP, National Crime Information Center (NCIC) and internal IRS and Department of Homeland Security, Immigration and Customs Enforcement (DHS/ICE) databases, revealed that MAYSSAMI is also known as Mohammad Meyssami, Moe Meyssami and Moe Meissami. His date of birth is November 25, 1956. He was born in the Islamic Republic of Iran and legally entered the U.S. to attend college in the 1970s.

I reviewed investigative reports by agents of the former United States Customs Service (now DHS/ICE), written during a 1992 investigation into the financial activities of numerous individuals in the San Jose area, including Mayssami. According to the reports, an undercover agent met with an individual named Mahmud Sharif, owner of Sharif Jewelers in Sacramento, California, to discuss the possibility of laundering money. Sharif told the undercover agent that he [Sharif] would be able to launder a small amount of money but that the agent should contact "...Moe Mayssami, San Jose, for larger amounts of money..." "Moe Mayssami" was later identified by agents as Mohammad Mayssami.

In April of 1992, Sharif and the undercover agent met with Mayssami in San Francisco, California, to discuss the laundering of money. The reports I reviewed detail conversations between Mayssami and the undercover agent[9].

Mayssami told the undercover agent that he owns a jewelry business and has numerous connections in the Middle East and Far East and that he [Mayssami] was ready to launder money for the agent anywhere in the world. According to additional reports in that case, the undercover agent attempted to arrange an appointment with Mayssami between September 1992 and January1993, but, due to scheduling difficulties, Mayssami and the undercover agent never met again. The reports do not indicate that Mayssami was ever arrested or charged with any offenses connected to the investigation, and Mayssami's criminal history does not indicate he has ever been arrested for money laundering.

---

[9] The reports do not indicate whether the conversation between the undercover agent and Mayssami was recorded

H. Visit by Law Enforcement Agents to the Premises to be Searched

On August 12, 2005, Special Agent Mary Hicok and I visited Mayssami Diamonds at 861 6th Avenue, Suite 175, in San Diego, California. Present at Mayssami Diamonds at the time of the visit was a female assistant whose name is unknown to me. Special Agent Hicok and I observed what appears to be a jewelry store carrying expensive high-end jewelry. I observed a retail sales area with a U-shaped counter containing necklaces, bracelets and other jewels, as well as what appeared to be an office behind the counter at the back of the store.

Special Agent Hicok identified herself and provided the female with a business card indicating that she worked for IRS-CI in San Jose, CA, and asked to speak to Mr. Mayssami. She told us that Mr. Mayssami was currently in Iran, and was expected back on September 1, 2005. Agent Hicok requested that she give the card to Mr. Mayssami when he returned to the U.S. and ask him to call her. The employee said she would do so. She asked what it was about, but Agent Hicok declined to tell her the purpose. She said that it was something that she wished to discuss only with Mr. Mayssami.

As we started to leave, Agent Hicok commented that the store had some lovely items to which the woman inexplicably responded "Yes, it is a dangerous business." We left without asking her to explain the comment.

I. September 2005 Customs Inspection of Mr. Mayssami

On August 19, 2005, I spoke with Special Agent Phil Young at DHS/ICE in San Jose via telephone. At my request Agent Young agreed to arrange for Mr. Mayssami to go through a secondary inspection upon his return to the United States. He also arranged to have either himself or me notified when Mr. Mayssami returned and presented himself for entry into the United States.

On September 3, 2005, at approximately 2 p.m. I received a phone call from Agent Young who reported that Customs and Border Protection Inspector Manley had called to notify him that Mayssami had returned to the U.S. via Los Angeles International Airport at approximately 1:30 p.m. that day. Inspector Manley reported that Mayssami had arrived at LAX on KLM Flight #601 from Amsterdam. Mayssami was traveling with his wife and children (Inspector Manley did not speak with the wife or children, only Mr. Mayssami). Mayssami was taken to secondary inspection and questioned about his activities overseas. According to the Inspector, Mayssami reported that he is a U.S. citizen who works as a wholesaler jewelry businessman. Mayssami reported that he had spent the last two months visiting family in Iran and traveling throughout Europe with his wife, son and daughter. Inspector Manley inspected Mr. Mayssami's luggage and all items Mr. Mayssami had on his person. Inspector Manley did not tell Agent Young that anything of interest was found. Mr. Mayssami had with him several business cards which Inspector Manley photocopied and provided to Agent Young and myself. One of the business cards was for "Mayssami Diamond." Printed on the Mayssami Diamond card is the name Moe Mayssami, Jewelry Exchange Building, 861 Sixth Ave., Ste. 175, San Diego, CA 92101, Tel: (619) 232-1130, Cell: (619)708-8884, Fax: (619)232-1124, E-mail: arashbatt@sbcglobal.net. Other business cards on Mayssami's person included a Jewelry Liquidators business card with an address in Woodland Hills, California and a business card for "Gordon James" with two California addresses an e-mail address but no company name or other information.

V. SUMMARY AND ANALYSIS

Based upon the foregoing, I believe that there is probable cause to believe that Mayssami aided Setayeshi and Supermicro Computer in committing violations of 50 U.S.C. § 1705(b), as well as the EAR and the OFAC embargo against Iran, by providing financing for the illegal shipment to Iran of computer products. This financing would not have been possible or legal through traditional banking channels.

I also believe that there is probable cause to believe that Mayssami has violated 18 U.S.C. § 1956 by using his business, Mayssami Diamonds, to conceal or disguise the nature, location and source of funds that represent the proceeds of some form of illegal activity within the meaning of 18 U.S.C. § 1956. As seen above, it appears that Mayssami had retail consumers who were purchasing jewelry from him make checks for the purchase of jewelry payable to Supermicro, or perhaps had them leave the payee blank and inserted "Supermicro" himself. He also had a hawala customer trying to purchase a condominium in Tehran deposit money into Supermicro's account via a wire transfer.

I also believe that it is unlikely that Supermicro and Setayeshi are Mayssami's only money laundering customers. Based on the U.S. Customs reports I read, he appears to have been doing this since at least 1992. Also, as seen above, Mayssami was known to another jeweler in California as someone to contact if you wanted to transfer money to Iran. Hawaladers typically do not have only one customer. And the fact that sending money to or from Iran for any commercial purpose is illegal would increase the demand for his services.

I therefore believe that there is probable cause to believe that, in addition to evidence of his assistance to Mr. Setayeshi and Supermicro, there will be evidence of other money laundering totally unrelated to the Supermicro investigation.

VI. PREMISES TO BE SEARCHED

Mayssami Diamonds is located at at 861 6th Avenue, Suite 175 in San Diego, California. The business is further described as follows.

It is located in the "Jewelers Exchange" building, an eight story concrete building at the corner of Sixth Avenue and E Street in San Diego. The exterior of the top six floors of the building are painted green and white with a red line separating the seventh and eighth floors. The entrance to the building consists of two sliding glass doors and is on the west side of the building, facing Sixth Avenue. Just above the entrance to the building is a green sign with the letters "Jewelers Exchange" written in gold with a picture of a diamond. Below the sign are the numbers "861," also in gold.

The building houses numerous businesses. Permission is only sought to search Suite 175. Suite 175 is located on the first floor on the north side of the building. The front of the suite is made entirely of glass and consists of two double glass doors with the words "Mayssami Diamonds Since 1948" written in white with a picture of a diamond and the words "By Appointment Only." A telephone number, "619-232-1130" is also written on the door. The suite number, "175" is also on the door, written in gold.

VII. ITEMS TO BE SEIZED

The allegations in this affidavit pertain to money laundering in violation of 18 U.S.C. § 1956 as well as violations of 50 U.S.C. §1705(b) and the related violations of the Export Administration Regulations and the Iran Transaction Regulations. The purpose of this search warrant is to search for evidence, both documentary and electronic, of possible money laundering and export violations that were engaged in by Mohammad Ali Mayssami at Mayssami Diamonds in San Diego, California.

Based on my training and experience, as well as conversations I have had with other agents, I believe that there is probable cause to believe that the types of evidence described below will be found at Mayssami Diamonds at 861 6th Avenue, Suite 175, in San Diego, California.

I believe this in part because money laundering, hawala, and the illegal export of goods all generally require that business records be kept. Without them it would impossible to keep track of who owes you money, who you owe money to, and the amounts involved. Without records it would be impossible to establish for a customer (*e.g.*, Supermicro) that a certain transaction has been made. And, as seen above, the crimes themselves sometimes use financial instruments, *e.g.*, personal checks, to commit the offense. And while hawala is more informal than regular banking channels, and operates without the use of written promissory instruments, this does not mean that a hawaladar can operate without records. He needs to be able to know what he is owed by other hawaladars and what other hawaldars owe him. I note that several of the emails quoted above mention Mr. Mayssami faxing confirmations of deposits to Supermicro and to Setayeshi. If he keeps records regarding his dealings with Setayeshi and Supermicro, there is no reason to think that he does not keep records regarding other money laundering customers as well.

I believe that these records will be found at Mayssami Diamonds, as opposed to somewhere else, because it is the only business address we have found in the U.S. for him; because we know that the otherwise legitimate business conducted by Mayssmai Diamonds appears to have been used to help launder money for Supermicro, Mr. Setayeshi, and probably others; and because, when agents visited the location, they observed what appeared to be a business office behind the sales floor.

Based on my training and experience, I therefore believe that there is probable cause to believe that the following records, in either hard copies or electronic versions, will be found at Mayssami Diamonds:

1. Records indicating transfers of payments, including hawala transfers, for illegal transactions from people in Iran to Mayssami, including: general account ledgers, accounts receivable ledgers, accounts payable ledgers and other ledgers of accounts concerning these completed or contemplated transactions; bank records such as statements, check stubs and registers, canceled checks, deposit tickets, debit memos, wire transfer documents, certified check memos, official cashier's checks memos, money orders, letters of credit, and bank drafts;

2. Records indicating all transfers of payments, including hawala payments, for illegal transactions from Mayssami to people in Iran, including all items mentioned in Item 1, above;

3. Records indicating transfers of payment from Mayssami to Supermicro, including all records mentioned in Item 1, above;

4. Records of the identities of customers of Mayssami whose checks or other financial instruments were used by Mayssami to launder funds for illegal commercial transactions with Iran, including cash receipts, sales receipts, and other records of purchase;

5. Records of the identities of other money laundering customers of Mayssami, including facsimile communications, electronic mail (e-mail) communications, correspondence, telephone messages, calendars, sales acknowledgments, general accounts, accounts receivable, accounts payable and other ledgers of accounts;

6. Correspondence, including electronic mail (email), all facsimile communication, correspondence, telephone messages, calendars, sales acknowledgments, technical specifications, internal memorandums, notes from meetings and conversations concerning completed or contemplated illegal transactions with people in Iran;

7. Correspondence, including electronic mail (email), all facsimile communication, correspondence, telephone messages, calendars, sales acknowledgments, technical specifications, internal memorandums, notes from meetings and conversations concerning completed or contemplated illegal transactions with people in the U.S., regarding payment for illegal commercial transactions with Iran.

VIII. PROPOSED SEARCH PROCEDURE FOR THE SEARCH OF ELECTRONICALLY STORED EVIDENCE

Based upon my training and experience, and conversations that I have had with other law enforcement officers who investigate export violations, I know that searches of premises containing the types of documentary evidence sought here commonly yield data stored in electronic format on memory calculators, computers, computer disks, and other electronic data storage media.

Based upon my knowledge, training and experience, and consultations with a computer forensics expert, I know that data and information stored in an electronic format may be found not only on the hard disk of a computer, but on other computer hardware, peripherals, and storage media, including back-up tapes, diskettes, CD-ROMs, handheld organizers, and other devices capable of storing information in an electronic format.

Additionally, searching and seizing information from computers often requires agents to seize most or all the computer hardware to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following.

(1) The Volume of Evidence.

Computer storage devices (like hard disks, diskettes, tapes, CD-ROMs, and Digital Video Disks (DVD's)) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; or might store it in many places and with deceptive file names. This may require authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process could take several weeks to conduct, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

(2) Technical Requirements

Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data.

(3) Files May be Password-Protected or Encrypted

The data search procedures used to recover electronically stored evidence are designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. However, without knowing the passwords for the encrypted files, it may be impossible to decrypt the files in order to view the information contained within the files. This is especially true of certain encryption algorithms/programs, which include PGP, Elgamal, RSA, Diffie-Hellman, DSA, DES, Gost Blowfish, CAST, IDEA, and Triple-DES. Other, less secure encryption methods may still require considerable time or outside agency assistance to decrypt the files absent a password.

(4) Danger of Destruction of Evidence

Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code embedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis and generally cannot be done on site.

A computer forensics expert also has advised me that searching computerized information for evidence or instrumentalities of crime commonly require agents to seize most or all of a computer's equipment including hardware, a system's peripheral, software, documentation, and passwords and data security devices so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following.

The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular peripheral (or "input/output") devices in order to read the data on the system. Also, certain operating systems and hardware can be configured to operate only with a precise set of hardware, software, and peripherals. In these instances, it is important that the analyst be able to properly reconfigure the system as it now operates in order to accurately retrieve evidence. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all relevant instruction manuals or other documentation and data security devices.

Therefore, it is requested that agents executing this search warrant be authorized to employ the following procedures upon execution of the search warrant.

Upon securing the premises, a computer forensics expert will make an initial review of any computer hardware, system peripherals, or storage media to determine if it is possible to search these items during the execution of the search warrant without jeopardizing our ability to preserve the electronically stored information in its original state. A computer forensics expert will also determine if, as an alternative to on-site inspection, it is possible to make bit-image backups of the original computer hardware and magnetic storage media (i.e. hard disk drives, diskettes, JAZ and ZIP disks) on site within a reasonable period of time, and if these backups will be useable for an offsite examination conducted at a later date without the original equipment. As stated above, some operating systems or hardware configurations require the original equipment to be present in order to access the information contained on the system.

If it is not possible to perform an on-site review of these materials or to create usable bit-image backups, the agents executing the warrant will be authorized ro seize all computer hardware, system peripherals, software, documentation, password and data security devices, and storage media as defined below. The seized items will be transported to an appropriate law enforcement facility for a timely analysis and review.

Any electronically stored information or data that does not fall within the list of items to be seized will be returned to the subject premises within 10 days from the execution of the warrant. However, any electronically stored information, data, image or file found to contain, or constituting, contraband (as defined by law), shall not be returned. Further, any and all encrypted files that cannot be reviewed absent a password, and where such password was not provided, shall not be returned.

Any computer equipment taken from the subject premises in order to perform an offsite search for electronically stored information and data shall be returned to the subject premises within 10 days from the execution of the warrant. If it is not possible to conduct the offsite examination within the 10 day time period, because of the volume of electronically stored information to be reviewed or the need for specialized equipment or expertise to conduct the review, your affiant may apply for a Court ordered extension of the 10 day time period.

Items which constitute evidence of the commission of a criminal offense or are contraband, the fruits of a crime, or things otherwise criminally possessed, or are property designed or intended for use or which is or has been used as the means of committing a criminal offense shall not be returned. We propose that agents may be allowed to seek forfeiture of these items according to law.

There is no indication that any "work product" or "documentary" materials are stored on the computer(s) to be searched that are being kept for the purpose of disseminating them to a public newspaper, broadcast, or other similar form of public communication. Should agents become aware of such materials as described in 42 U.S.C. § 2000aa, they shall be returned as quickly as circumstances permit without being copied or seized.

For purposes of this warrant, the foregoing terms are defined as follows:

Hardware: Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, self contained "laptop" and "notebook" computers, hand-held electronic organizers, and "personal digital assistants"), internal and external storage devices (magnetic storage devices such as hard disk drives, diskette drives, and tape drives, optical storage devices such as CD-ROM drives, CD-R/CD-RW recorders, and DVD drives/recorders, and other memory storage devices), and related communications devices such as modems, cables and connectors, programmable telephone dialing or signaling devices, and electronic tone generating devices, as well as any devices, mechanisms or parts that can be used to restrict access to computer hardware such physical keys and locks.

System Peripherals: A piece of equipment which sends data to, or receives data from, a computer. Keyboards, mouses, printers, scanners, plotters, video display monitors, and certain types of facsimile machines are examples of peripherals.

Software: Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

Documentation: Computer related documentation consists of written recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass phrase (a string of alphanumeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, cards, and circuit boards. Data security software of digital code may include a programming code that creates "test" keys or "hot" keys, which perform certain preset security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it. Storage Media.

Storage media includes any material capable of storing information in a manner that can be used by computer hardware to save and/or retrieve information. Examples of storage media include diskettes, CD-ROMs, DVD's, magnetic tapes, ZIP disks, JAZ disks, and EPROMS.

ERIN D. KELLY
Special Agent
U.S. Department of Commerce

Subscribed and sworn to me this 29th day of September, 2005, in San Diego, California.

HON. WILLIAM MCCURINE JR.
United States Magistrate Judge